INDIAN INSTITUTE OF TECHNOLOGY BOMBAY

MATERIALS MANAGEMENT DIVISION

Powai, Mumbai 400076

For RFx No.6100000381 (PR No.1000015079)

Technical Specifications of "Supply, Installation and Testing of Next Generation Firewall"

Quantity: 2 units in HA mode

a) Pre-Qualification Criteria: (Responses to be uploaded in Technical bid)

1. The Bidder should be a Company registered under the Companies Act 1956, or Limited Liability Partnership formed as per the Limited Liability Partnership Act 2008, for the last three years. (Copy of Certificate of Incorporation/Registration of the firm Certificate must be uploaded on technical bid).

2. Participating Bidders should be providing Proposed Services to at least 2 Customers in India. (Copy of Purchase orders/work orders to be uploaded in technical bid)

3. The Bidder should have authorization from the OEM to quote their products, and should be authorized business and Service partner of the OEM. (Authorization Letter from OEM and/or Self Declaration must be uploaded on technical bid).

4. All the bidders/OEMs should be fully comply with all the requirements mentioned in this tender to be able to qualify. No deviation letter on company's letterhead for this tender to be uploaded on technical bid.

b) General Requirements

1 The proposed solution must provide Layer 7 / application Layer security solution. The solution must be deployed in HA mode at IIT. The Firewall must support application identification natively, without requiring any license/subscription/blade. IIT must not be required to buy any license for application visibility and these must operate at Layer 7 natively.

2 "The proposed application security solution must be in the must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive 5 years"

3 For high performance with low latency the proposed solution must provide all application level inspection as real-time stream-based and not using file-based store-and-forward techniques

4 The proposed vendor must have a "Recommended" rating with min 99% Evasion proof capability and min 97.5% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Test Report.

5 The proposed solution must allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters.

6 "The proposed solution shall support packet captures based on:

-Applications
-Unknown Applications
-any threat
-data-filters"

7 The proposed appliance must have at least 12 x 1G copper Ports, 4 x 1Gig SFP fibre & 4 x 10G SFP+ fibre - ports from day one.

8 The proposed appliance must have 1 x 1G port for out of band management. Also 1x 10G SFP+ port for HA connectivity to sync config / session between HA pairs. These ports must be in addition to production ports mentioned earlier.

c) Performance

9 The proposed solution will be a Next Generation Firewall and not an UTM (unified threat management) system, with a capability of supporting at least 4.3 Gbps of Application Identification Enabled Firewall throughput using 64KB of transaction size for HTTP/Appmix traffic. The OEM must publish performance claims on public domain like websites, datasheets.

10 The proposed solution must provide 2 Gbps of throughput with all security features enabled including application Control, IPS, antivirus, anti-spyware, APT, and logging enabled, utilizing 64 KB HTTP/appmix transactions. The performance must be based on HTTP traffic and not UDP. The OEM must publish performance claims on public domain like websites, datasheets.

11 The proposed solution must be able to handle upto 55,000 new sessions per second

12 The proposed solution must be able to handle up to 1.000,000 concurrent sessions

13 The solution must be capable of handling upto 8,000 policies

14 The proposed solution must be able to handle upto 2.5 Gbps IPSEC VPN throughput

15 The proposed solution must support a minimum 500 Site to Site IPSEC VPN tunnels. The proposed solution must support a minimum 1,000 clients to site VPN tunnels for windows, Mac and linux machines . All licenses need to be provisioned from day one.

The proposed firewall should also support host information profiling to comply with the VPN user before accessing the network. This is used to collect information about the security status of the endpoints -- such as whether they have the latest security patches and antivirus definitions. installed, whether they have disk encryption enabled, or whether it is running specific software

you require within organization. This information can then be used in security policies to decide if the endpoint is allowed to access a specific resource or not. This is required from day 1.

d) Operation Mode

16 The proposed solution must support Tap Mode, Transparent, Layer 2 , Layer 3 mode providing flexible deployment. The proposed solution must be able to support simultaneous deployment with interfaces servicing Layer 3, Layer 2, Transparent and Tap modes.

17 The proposed solution must support 802.1Q VLAN tagging

18 The proposed solution must support Dual Stack IPv4 & IPv6 application control and threat inspection under various deployment modes from day one.

19 The proposed solution must support standards based Link aggregation (IEEE 802.3ad) to achieve higher bandwidth

20 The proposed solution must support logical Ethernet subinterfaces tagged and untagged.

21 The proposed solution must support the following routing protocols static, RIPv2, OSPF, BGP4

22 The proposed solution must have Virtual Router capabilities that supports all L3 capabilities. The proposed solution must have IPv6 Static Routing Support even for virtual routers.

23 The proposed solution must support DHCPv4 and DHCPv6 relay from day one.

24 High Availability

25 The proposed solution must be able to support Active/Active HA configuration

26 The proposed solution must be able to support Active/Passive HA configuration

27 The proposed solution must be capable to detect device, link and path failure

28 The proposed solution must be able to support session and configuration synchronization

29 The proposed solution must synchronize the following for HA. Sessions, Decryption Cert, Threat and application Signature etc ensuring seamless operations

30 The OEM must provide 24 X 7 X 365 technical support. The OEM must provide the dedicated login credentials to IIT with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. IIT should be able to raise tickets directly to OEMs.

31 Every Gateway Security control (like Firewall or any other feature required to meet above specification) must not have any restriction on number of users and must be supplied for unlimited users unless specified otherwise.

32 The proposed solution must support load balancing multiple internet links.

e) Firewall Security policy

33 The proposed solution must support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic from day one. The proposed solution must have application and application function identification and decoding technology from day one.

34 The proposed solution must be able to handle unknown/unidentified applications e.g. alert, block or allow

35 The proposed solution must be able to create custom application signatures and categories based on the IIT environment.

36 The proposed solution must delineate specific instances of peer2peer traffic (Bittorrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.).

37 The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.

38 The proposed solution must support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)

39 The proposed solution must support authentication services for user-identification using any of the following technologies AD, LDAP, eDirectory, Radius, Kerberos, Client Certificate from day one.

40 The proposed solution must support the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP.

41 The proposed solution must support user-identification in policy without installing an agent on individual endpoints.

42 The proposed solution must support user-identification over wireless by integrating with Wireless controllers.

43 The proposed solution must populate and correlate all logs with user identity (traffic, IPS, URL, data, etc.) without any additional products or modules in real-time

44 The Firewall must provide NAT functionality, including dynamic and static NAT translations.

45 Network address translation (NAT) must be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.

46 Network Address Translation (NAT) must be configured as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT must be supported.

47 Port address translation must be provided

48 The proposed solution must support Policy Based forwarding based on Zone, applications , Source / Destination Address, User or User Group

f) Threat Prevention Features

49 The proposed solution shall support IPS , Anti Virus and Anti Bot & Spyware Protection features from day one.

50 The proposed solution shall be supported by a world-class threat research organization dedicated to the discovery and analysis of threats, applications and their respective network behavior. The threat and vulnerability information that is protected shall be publicly accessible on the internet.

51 The proposed solution shall block known network and application-layer vulnerability exploits

52 The proposed solution shall block buffer overflow, DoS/DDoS , etc type of attacks

53 The proposed solution shall perform stream-based Anti-Virus & Anti-Spyware and not store-and-forward traffic inspection

54 The proposed solution shall support attack recognition for IPv6 traffic the same way it does for IPv4

55 The proposed solution shall support Built-in Signature and Anomaly based Vulnerability Protection Engine

56 The proposed solution shall support the ability to create custom user-defined signatures

57 The proposed solution shall support granular tuning with option to configure overrides for individual signatures

58 The proposed solution shall support automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)

59 The proposed solution Vulnerability / Virus / Spyware protection signature updates shall not require reboot of the unit.

60 The proposed solution must support different actions in the policy such as deny, drop, reset client, reset server, reset both client and server.

61 Integrated IPS, Antivirus, Anti-Spyware & Anti-Bot functionality should be available as a module that can be activated and deactivated as and when required.

62 Activation of new IPS protections should be based on parameters like Threat severity i.e. High, Medium, low risk etc.

63 IPS Profile should have an option to select or re-select specific signatures that can be deactivated.

64 The proposed solution must have an option to add exceptions for network, services and Users.

65 The proposed solution must have functionality of Geo Protection to Block the traffic country wise.

66 The proposed solution must have an option to create your own signatures with an open signature language.

67 The proposed solution must provide detailed information on each protection, including: Vulnerability and threat descriptions, including CVE details & Threat severity

68 Solution must be able to identify malwares coming from incoming files and malwares downloaded from Internet

69 Solution must be able to discover bot outbreaks

70 Solution must be able to discover the Bot infected machine

71 Solution must be able to prevent bot damage

72 Solution must have an Multi tier bot discovery ie Detect Command and Control IP/URL and DNS

73 Solution must be able to detect unique communication patterns used by Botnets.

74 Solution must be able to block traffic between infected Host and Remote Operator and not to legitimate destination

75 Solution must be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc

g) SSL and SSH Decryption must be supported from day 1

76 The proposed solution shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)

77 The proposed solution shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection

78 The proposed solution must support decryption and inspection of SSL traffic in an outbound connection, inbound connection across any port.

79 The proposed solution shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic

80 The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.

81 The proposed must support on appliance SSL decryption policy based on IP, User, web category.

h) Anti APT (Sandboxing) Features should be supported whenever required in future on same appliance by license up-gradation (with one exception in clause 90 about EXE file types)

82 The proposed solution must provide an on-cloud APT solution to analyse unknown files.

83 The proposed solution must support behaviour based inspection and protection of unknown viruses and zero-day malware for any application and protocol including SMTP, HTTP, SSL, POP, IMAP etc.

84 The proposed solution must support extraction of unknown files from above mentioned protocols and forward to APT cloud for detailed analyses without any manual intervention

85 The proposed solution must support automated signature generation for discovered zero-day malware and the OEM should update these prevention signatures every 5 mins.

86 Solution must perform sandbox based multi-version analysis including OS like Windows XP & Windows 7, Adobe Acrobat & Flash.

87 The proposed solution must support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware

88 The solution must support a minimum four levels of decompression/decoding for any combination of decoding: ZIP, gzip, base64,chunked, uuencode.

89 The solution must provide the ability to block files with multi-level-encoding with 4 or more levels of compression e.g office file in 4 levels of zip.

90 The solution must provide the ability to scan PE, Office, PDF, Java, Flash, APK etc in sand boxing environment to inspect for malware. EXE files sandboxing is required from day 1. Please consider any license if required for exe file types

91 The Proposed solution must support Multiple OS in Sand Boxing environment including Windows XP, Windows 7 (32/64) etc versions. The proposed solution also must support "Bare Metal Analysis on cloud"

92 The proposed solution must provide a minimum 4 signatures to block malware spread in the network, post APT analyses, to stop repeat incidents, C2C communication & infected host identification. 4 Signature must include Antivirus, URL, DNS & Anti C2C Communications

93 The solution must provide support for XFF to identify end user behind Proxy servers

94 The solution must provide support for DNS sinkholing to identify end users trying to resolve malicious domains sitting behind internal DNS servers.

95 The solution should be able to identify and block traffic that doesn't match any known application or when using a non-default port for the application.

96 Solution should be able to block the transfer of specific file types, I.e. PE files transferred regardless of the port, protocol or application used. It should be able to create different policies for different user groups.

i) Following URL Filtering should be supported wherever required in future on same appliance by license up-gradation

97 The proposed solution shall support URL-Filtering with categories and should have "Malware URL category"

98 The Proposed solution shall have the database located locally/ cache url category on the device

99 The proposed solution shall support custom URL-categorization

100 The proposed solution shall support customizable block pages

101 The proposed solution shall support logs populated with end user activity reports for site monitoring within the local solution

102 The proposed solution shall support Drive-by-download control

103 The proposed solution shall support URL Filtering policies' by AD user, group, machines and IP address/range

j) QOS

104 The proposed firewall must support the ability to create QoS policy

105 by destination address

106 by user/user group as defined by AD

107 by application (such as Skype, Bit torrent, YouTube, azureus)

108 by static or dynamic application groups (such as Instant Messaging or P2P groups)

109 The proposed firewall must define QoS traffic classes with:

110 guaranteed bandwidth

111 maximum bandwidth

112 priority queuing

113 The proposed firewall must support real-time bandwidth statistics of QoS classes.

k) Management & Reporting

114 Must support on-box logging and reporting without need of any central management console or tool.

115 Firewall must support the user based logging.

116 It must be able to correlate logs from various modules such as Firewall, Application Control, Antivirus & information at different periods of Time.

117 It must support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.

118 The firewall must be capable of integrating with other equipment like SIEM tool or reporting tools etc.

119 NGFW must have on-box Automated Correlation Engine to provide areas of risks and compromised hosts on network

120 The proposed solution shall populate and correlate all logs with user identity (traffic, IPS, URL, data, AV,AB etc.) without any additional products or modules in real-time

121 NGFW must have on-box application based, threat based reports without need of any additional appliance or tool

122 NGFW must have an “automated correlation engine” on the firewall itself to correlate multiple types of logs and identify infected hosts.

123 Proposed NGFW must be Common criteria EAL4/NDPP certified.

l) Warranty and License Support

124 All Products Warranty and License Support to be for 3 Years, with OEM premium support.